

ON GOPPA CODES ON THE HERMITIAN CURVE

E. BALLICO AND A. RAVAGNANI

ABSTRACT. Here we study the dual of some m -point Goppa codes on the Hermitian curve (their minimum distance and the description of all the codewords with minimum weight).

1. INTRODUCTION

Let K be a finite field and C a geometrically connected smooth projective curve. Fix any line bundle $\mathcal{L} = \mathcal{O}_C(D)$, $D > 0$, on C defined over K and any $B \subset C(K)$, with B disjoint from the support of D . Let $\mathcal{C}(B, \mathcal{L})$ denote the Goppa code obtained evaluating the rational functions f on C with $(f)_\infty \leq D$ at the points of B . Now assume $C \subset \mathbb{P}^r$, that C is a complete intersection and that $\mathcal{L} \cong \mathcal{O}_C(d)$ for some d . With these assumptions A. Couvreur found a lower bound for the minimum distance of the dual code $\mathcal{C}(B, \mathcal{O}_C(d))^\perp$ in terms of d and the projective geometry of B (e.g. the existence of $d+2$ collinear points of B) ([2]). In this paper we extend Couvreur's approach to more general line bundles. We use it for the Hermitian curve and for m -points codes on it, $m \geq 3$. One-point codes on a Hermitian curve are well-studied and efficient methods to decode them are known ([17], [18], [19]). The minimum distance of two-point codes on a Hermitian curve is known ([6], [7], [8], [9], [14]). See [15], [4] for a description of the codewords with minimum weight for some one-point code on the Hermitian curve, the latter paper using [2]. The main task in this paper is to get a description of all the codewords with minimum weight for certain m -point codes, $m \geq 3$, but as far as we know not even the minimum distance was known (although it is easier to get it). For a similar, but more refined, study of two-point codes on the Hermitian curve, see [16]. For the second and the third Hamming weight for one-point codes on the Hermitian curve, see [12], [19], [13]. For the second Hamming weight for two-point codes on the Hermitian curve, see [10].

Theorem 1. *Assume $K = \mathbb{F}_{q^2}$ and take as C the Hermitian curve. Fix $P_1, P_2, P_3 \in C(\mathbb{F}_{q^2})$ such that $P_i \neq P_j$ for all $i \neq j$, and P_1, P_2, P_3 are not collinear. Take $B := C(\mathbb{F}_{q^2}) \setminus \{P_1, P_2, P_3\}$. Fix an integer $d \geq 5$ such that $1 \leq d \leq q-1$ and integers $a_i \in \{1, \dots, d\}$, $1 \leq i \leq 3$, such that $a_1 + a_2 + a_3 \leq 3d-5$ and $a_i = d$ for at most one index i . Set $E := a_1P_1 + a_2P_2 + a_3P_3$. Let \mathcal{C}^\perp be the dual of the code $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(d)(-E))$. \mathcal{C} is an $[n, k]$ -code with $n = q^3 - 2$ and $k = \binom{d+2}{2} - a_1 - a_2 - a_3$. Let L_i , $1 \leq i \leq 3$, be the line spanned by P_j and P_h with $\{i, j, h\} = \{1, 2, 3\}$. Then \mathcal{C}^\perp has minimum distance d and the codewords with minimum weight are exactly the ones whose support is formed by d points of $B \cap L_i$ for some $i = 1, 2, 3$.*

1991 *Mathematics Subject Classification.* 14G15; 14H99.

Key words and phrases. Hermitian curve; Goppa code; m -point code.

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

Theorem 1 is false if we take $a_1 = a_2 = d$ and $a_3 > 0$ (Remark 3).

Theorem 2. *Assume $K = \mathbb{F}_{q^2}$ and take as C the Hermitian curve. Fix integers s, d, a_i , $1 \leq i \leq s$, such that $2 \leq s \leq d-1 \leq q-2$, $0 < a_i \leq d+1-i$ for all i and $a_1 + \dots + a_s \leq 3d-7+s$. Fix s distinct collinear points $P_1, \dots, P_s \in \mathcal{C}(\mathbb{F}_{q^2})$. Call R the line containing the s points P_1, \dots, P_s . Take $B := \mathcal{C}(\mathbb{F}_{q^2}) \setminus \{P_1, \dots, P_s\}$. Set $E := \sum_{i=1}^s a_i P_i$, $n := q^3 + 1 - s$ and $k := \binom{d+2}{2} - a_1 - \dots - a_s$. The code $\mathcal{C} := C(B, \mathcal{O}_C(d)(-E))$ is an $[n, k]$ -code with minimum distance $d+2-s$ and the codewords of \mathcal{C}^\perp with minimum weight are exactly the one whose support, S , is formed by $d+2-s$ points of $B \cap R$. Any $S \subseteq R \cap B$ with $\sharp(S) = d+2-s$ is the support of exactly one (up to a non-zero scalar) codeword with minimum weight.*

G. L. Matthews computed the Weierstrass semigroup of any s collinear points of $\mathcal{C}(\mathbb{F}_{q^2})$ ([11]). Hence the dimensions of all $H^0(C, \mathcal{O}_C(t)(-\sum_{i=1}^s a_i P_i))$, any t , any $a_i \geq 0$, are known.

If we restrict the set B we get dual codes \mathcal{C}^\perp with better parameters.

Theorem 3. *Take the set-up of Theorem 1, but with $a_1 \geq a_2 \geq a_3 > 0$, $a_1 + a_2 \leq 2d-2$, $B' := \mathcal{C}(\mathbb{F}_{q^2}) \setminus (C(\mathbb{F}_{q^2}) \cap (L_1 \cup L_2 \cup L_3))$ and $\mathcal{C} := C(B', \mathcal{O}_C(d)(-E))$. Then \mathcal{C} is an $[n, k]$ -code with $n = q^3 - 3q + 1$ and $k := \binom{d+2}{2} - a_1 - a_2 - a_3$. Let \mathcal{S} be the set of all lines defined over \mathbb{F}_{q^2} through one of the points P_1, P_2, P_3 , but different from L_1, L_2, L_3 and from the tangent lines L_{C, P_i} , $i = 1, 2, 3$, of C at P_i . Let $\mathcal{S}(d+1)$ denote the set of all $S \subset B$ such that $\sharp(S) = d+1$ and S is contained in some line $L \in \mathcal{S}$. We have $\sharp(\mathcal{S}(d+1)) = 3(q^2 - 2)\binom{q}{d+1}$. The minimum distance of \mathcal{C}^\perp is $d+1$ and for each $S \in \mathcal{S}(d+1)$ there is a codeword (unique up to a scalar) with S as its support and with minimum weight. If $d \geq 6$ and $a_1 + a_2 + a_3 \leq 3d-6$, then all the codewords of \mathcal{C}^\perp with minimum weight arise in this way from a unique $S \in \mathcal{S}(d+1)$.*

See Theorem 4 for the set-up of Theorem 2 in which instead of B we take $B_1 := C(\mathbb{F}_{q^2}) \setminus R \cap C(\mathbb{F}_{q^2})$.

In all our results we assume $a_i \leq d$, for all i , while it would be more interesting to assume $0 \leq a_i \leq q$ (these are the cases necessary to describe all m -points codes on a Hermitian curve). We may reduced the case $a_i > d$ to the stated case, but decreasing if necessary d (see Remark 2 and Lemma 5).

2. ARBITRARY CURVES

Lemma 1. *Fix a smooth plane curve $C \subset \mathbb{P}^2$, an integer $x > 0$, a zero-dimensional scheme $E \subset C$ and a finite subset $B \subset C$ such that $B \cap E_{\text{red}} = \emptyset$. Set $\mathcal{C} := C(B, \mathcal{O}_C(x)(-E))$ and $c := \deg(C)$. Assume $\sharp(B) > xc - \deg(E)$. Set $n := \sharp(B)$, and $k := h^0(C, \mathcal{O}_C(x)) - \deg(E) + h^1(\mathbb{P}^2, \mathcal{I}_E(x))$, where $h^0(C, \mathcal{O}_C(x)) = \binom{x+2}{2}$ if $x < c$ and $h^0(C, \mathcal{O}_C(x)) = \binom{x+2}{2} - \binom{x-c+2}{2}$ if $x \geq c$. Then \mathcal{C} is an $[n, k]$ -code and the minimum distance of \mathcal{C}^\perp is the minimal cardinality, z , of a subset of B such that $h^1(\mathbb{P}^2, \mathcal{I}_{S \cup E}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_E(x))$. A codeword of \mathcal{C}^\perp has weight z if and only if it is supported by $S \subseteq B$ such that $\sharp(S) = z$, $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_E(x))$ and $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S'}(x))$ for all $S' \subsetneq S$.*

Proof. The computation of $h^0(C, \mathcal{O}_C(x))$ is well-known. We imposed that B does not intersect the support of E . The case $E = \emptyset$ is a particular case of [2], Proposition 3.1. In the general case notice that \mathcal{C} is obtained evaluating a family of homogeneous

degree x polynomials (the ones vanishing on the scheme E) at the points of B . Since C is projectively normal, the restriction map $\rho_x : H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(x)) \rightarrow H^0(C, \mathcal{O}_C(x))$ is surjective. Hence the restriction map $\rho_{x,E} : H^0(\mathbb{P}^2, \mathcal{I}_E(x)) \rightarrow H^0(C, \mathcal{O}_C(x)(-E))$ is surjective. Hence a finite subset $S \subset C \setminus E_{red}$ imposes independent condition to $H^0(C, \mathcal{O}_C(x)(-E))$ if and only if S imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(x))$. S imposes independent conditions to $H^0(\mathbb{P}^2, \mathcal{I}_E(x))$ if and only if $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(x)) = h^1(\mathbb{P}^2, \mathcal{I}_E(x))$ (here we use again that $S \cap E = \emptyset$). To get the existence of a non-zero codeword with support on S (not only with support contained in S) we need that the submatrix M_S of the parity check matrix associated to \mathcal{C} has the property that each of its submatrices obtained deleting one row have the same rank (each such row is associated to some $P \in S$ and we require that the codeword has support containing P). \square

Notice that we may drop the assumption “ $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S'}(x))$ for all $S' \subsetneq S$ ” in the statement of Lemma 1 if there is no $A \subset B$ such that $\#(A) < z$ and $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup A}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_E(x))$. This is the case when z is at most the Hamming distance of \mathcal{C}^\perp .

Remark 1. Take the set-up of the proof of Lemma 1. Since the restriction maps ρ_x and $\rho_{x,E}$ are surjective, the condition “ $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_E(x))$ ” is equivalent to the condition “ $h^0(C, \mathcal{O}_C(d)(-(E \cup S))) > h^0(C, \mathcal{O}_C(d)(-E)) - \#(S)$ ” or, equivalently (Riemann-Roch) $h^1(C, \mathcal{O}_C(d)(-(E \cup S))) > h^1(C, \mathcal{O}_C(d)(-E))$. In the applications we will usually have $d \leq \deg(C) - 3$ and hence $h^1(C, \mathcal{O}_C(d)) > 0$.

We recall the following particular case of [3], Corollaire 2. Parts (a) and (b) of Lemma 2 also follows in an arbitrary projective space from [1], Lemma 34. Parts (b), (c) and part (d) of Lemma 2 are just [3], Remarques at page 116.

Lemma 2. Fix integers $d > 0$ and a zero-dimensional scheme $Z \subset \mathbb{P}^2$ such that $\deg(Z) = z$.

- (a) If $z \leq d + 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) = 0$.
- (b) If $d + 2 \leq z \leq 2d + 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if there is a line T_1 such that $\deg(T_1 \cap Z) \geq d + 2$.
- (c) If $2d + 2 \leq z \leq 3d - 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \geq d + 2$ or there is a conic T_2 such that $\deg(T_2 \cap Z) \geq 2d + 2$.
- (d) Assume $z = 3d$. Then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \geq d + 2$ or there is a conic T_2 such that $\deg(T_2 \cap Z) \geq 2d + 2$ or there is a plane cubic T_3 such that Z is the complete intersection of T_3 and a plane curve of degree d .
- (e) Assume $z \leq 4d - 5$. Then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$ if and only if either there is a line T_1 such that $\deg(T_1 \cap Z) \geq d + 2$ or there is a conic T_2 such that $\deg(T_2 \cap Z) \geq 2d + 2$ or there are $W \subseteq Z$ with $\deg(W) = 3d$ and plane cubic T_3 such that W is the complete intersection of T_3 and a plane curve of degree d or there is a plane cubic C_3 such that $\deg(C_3 \cap Z) \geq 3d + 1$.

Proof. Since Z is zero-dimensional, for every $x \in \mathbb{Z}$ and any closed subscheme $W \subseteq Z$, we have $h^1(Z, \mathcal{I}_{W,Z}(x)) = 0$. Hence the restriction map $H^0(Z, \mathcal{O}_Z(x)) \rightarrow H^0(W, \mathcal{O}_W(x))$ is surjective. Hence if $h^1(\mathbb{P}^2, \mathcal{I}_W(d)) > 0$, then $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$. Take any integer $y \in \{1, \dots, d - 1\}$ and any degree y plane curve D_y (we allow the case in which D_y has multiple components). Set $W := D_y \cap Z$. From the exact

sequence

$$(1) \quad 0 \rightarrow \mathcal{O}_{\mathbb{P}^2}(d-y) \rightarrow \mathcal{O}_{\mathbb{P}^2}(d) \rightarrow \mathcal{O}_{D_y}(d) \rightarrow 0$$

we get $h^0(D_y, \mathcal{O}_{D_y}(d)) = \binom{d+2}{2} - \binom{d-y+2}{2}$ and that the restriction map $\rho : H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \rightarrow H^0(D_y, \mathcal{O}_{D_y}(d))$ is surjective. Hence if $h^0(D_y, \mathcal{I}_W(d)) > \binom{d+2}{2} - \binom{d-y+2}{2} - \deg(W)$, then $h^1(\mathbb{P}^2, \mathcal{I}_W(d)) > 0$ and hence $h^1(\mathbb{P}^2, \mathcal{I}_Z(d)) > 0$. Since $h^0(D_y, \mathcal{I}_W(d)) \geq 0$, we get $h^1(\mathbb{P}^2, \mathcal{I}_W(d)) > 0$ if $\deg(W) > \binom{d+2}{2} - \binom{d-y+2}{2}$. For $y = 1, 2$ it is sufficient to assume $\deg(W) \geq yd+2$. For $y = 3$ it is sufficient to assume $\deg(W) \geq 3d+1$. Now take $y = 3$ and $\deg(W) = 3d$. We have $h^0(D_3, \mathcal{I}_W(d)) > \binom{d+2}{2} - \binom{d-3+2}{2} - \deg(W)$ if and only if $h^0(D_3, \mathcal{I}_W(d)) > 0$, i.e. (by the surjectivity of ρ) if and only if there is a degree d plane curve C_3 such that $W = D_3 \cap C_3$. Hence in parts (b), (c), (d) and (e) we proved the “if” part. Now we check part (a) and the “only if” part of (b), (c), (d) and (e).

Let τ be the maximal integer such that $h^1(\mathbb{P}^2, \mathcal{I}_Z(t)) > 0$ (it exists, because $h^1(\mathbb{P}^2, \mathcal{I}_Z(t)) = 0$ for $t \gg 0$ by a theorem of Serre). By assumption we have $\tau \geq d$. Fix a positive integer $s \in \{1, 2, 3, 4\}$ and assume $\tau \geq s - 3 + z/s$. By [3], Corollaire 2, either $\tau = s - 3 + z/s$ and Z is the complete intersection of a degree s plane curve and a degree τ curve or there are $W \subseteq Z$ and an integer $t \in \{1, \dots, \tau - 1\}$ such that $\deg(W) \geq t(\tau - t + 3)$ and W is contained in a plane curve of degree t .

(i) Parts (a) and (b) are just the plane case of [1], Lemma 34.

(ii) Now assume $d + 2 \leq z \leq 2d + 1$. Since $\tau \geq d$, we have $\tau \geq d - 2$. Take $s = 1$. Since $\tau \geq d$, we have $\tau \geq 1 + 3 + z$. Hence we may apply [3], Corollaire 2, and get the existence of $W \subseteq Z$ and a line T_1 such that $\deg(W) \geq d + 2$ and $W \subset T_1$.

(iii) Now assume $2d + 2 \leq z \leq 3d$. Since $\tau \geq d \geq 3 - 3 + z/3$, we may apply [3], Corollaire 2, with the integer $s := 3$ and get parts (c) and (d).

(iv) Now assume $3d + 1 \leq z \leq 4d - 5$. Since $\tau \geq d > 4 - 3 + z/4$, we may apply [3], Corollaire 2, and get part (e). \square

3. THE HERMITIAN CURVE

From now on in this paper we take $K = \mathbb{F}_{q^2}$ and take as C the Hermitian curve ([17], Example VI.3.6). We have $\sharp(C(\mathbb{F}_{q^2})) = q^3 + 1$ ([17], p. 250, or [5]). For any $P \in C(\mathbb{F}_{q^2})$ let $L_{C,P} \subset \mathbb{P}^2$ denote the tangent line to C at P . Obviously $L_{C,P}$ is a line defined over \mathbb{F}_{q^2} . $L_{C,P}$ has order of contact $q + 1$ with C at P . Since $\deg(C) = q + 1$, Bezout theorem gives that $L_{C,P}$ meets C only at P .

Lemma 3. *Fix an integer $e \in \{2, \dots, q + 1\}$ and $P \in C(\mathbb{F}_{q^2})$. Let $E \subset C$ be the divisor eP seen as a closed degree e subscheme of \mathbb{P}^2 . Let $T \subset \mathbb{P}^2$ any effective divisor (i.e. a plane curve with perhaps multiple components) of degree $\leq e - 1$ containing E . Then $L_{C,P} \subseteq T$, i.e. $L_{C,P}$ is one of the components of T .*

Proof. Since $L_{C,P}$ has order of contact $q + 1 \geq e$ with C at P , we have $E \subset L_{C,P}$. Since $\deg(E) > \deg(T)$ and $E \subseteq T \cap L_{C,P}$, Bezout theorem implies $L_{C,P} \subseteq T$. \square

Lemma 4. *Fix integers $d \geq s \geq 1$, $P_i \in C(\mathbb{F}_{q^2})$, $1 \leq i \leq s$, such that $P_i \neq P_j$ for all $i \neq j$, and integers b_i , $1 \leq i \leq s$, such that $0 \leq b_i \leq d + 2 - i$ for all i and $b_i \leq q + 1$ for all i . Let $E := \sum_{i=1}^s b_i P_i$ be the degree $b_1 + \dots + b_s$ effective divisor of C . See E also as a degree $b_1 + \dots + b_s$ zero-dimensional subscheme of \mathbb{P}^2 . Then $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$.*

Proof. For any integer $j \in \{1, \dots, s\}$ set $E[j] = \sum_{i=j}^s b_i P_i$ and $E_i := b_i P_i$. Hence $E[1] = E$ and $E[i] = \sqcup_{i \leq j \leq s} E_j$. See each $E[i]$ as a degree $b_i + \dots + b_s$ zero-dimensional subscheme of \mathbb{P}^2 . Since L_{C, P_i} has order of contact $q+1$ with C at P_i and $b_i \leq q+1$, we have $E_i \subset L_{C, P_i}$. Hence $E[i+1] = E[i] \setminus E[i] \cap L_{C, P_i}$ for all $i = 1, \dots, s-1$. Seen $E[i]$ and $E[i+1]$ as zero-dimensional subschemes of \mathbb{P}^2 and L_{C, P_i} as a degree 1 curve of \mathbb{P}^2 , for any $t \in \mathbb{Z}$ and any $i \in 1, \dots, s$ we get an exact sequence of coherent sheaves on \mathbb{P}^2 :

$$(2) \quad 0 \rightarrow \mathcal{I}_{E[i+1]}(t-1) \rightarrow \mathcal{I}_{E[i]}(t) \rightarrow \mathcal{I}_{E_i, L_{C, P_i}}(t) \rightarrow 0$$

in which we see E_i as a degree b_i divisors of $L_{C, P_i} \cong \mathbb{P}^1$. Hence $h^1(L_{C, P_i}, \mathcal{I}_{E_i, L_{C, P_i}}(t)) = 0$ for all $t \geq b_i + 1$. Taking $t = d$ and $i = 1$ in (2) we get $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) \leq h^1(\mathbb{P}^2, \mathcal{I}_{E[2]}(d-1))$. If $s = 1$, we are done, because $E[2] = \emptyset$ in this case. In the general case we use induction on s . Notice that we may apply the inductive assumption to $E[2]$ with respect to the integer $d' := d - 1$. Hence the inductive assumption gives $h^1(\mathbb{P}^2, \mathcal{I}_{E[2]}(d-1)) = 0$. Use the long cohomology exact sequence of the case $t = d$ and $i = 1$ of (2). \square

Remark 2. Fix an integer $s \geq 2$, s distinct points $P_1, \dots, P_s \in C(\mathbb{F}_{q^2})$ and integers a_i, b_i , $1 \leq i \leq s$. Set $c := \sum_{i=1}^s b_i$, $E := \sum_{i=1}^s a_i P_i$, $G := \sum_{i=1}^s (b_i(q+1) - a_i)P_i$ and $G' := (c(q+1) - a_1)P_1 - \sum_{i=2}^s a_i P_i$. For any $P \in C(\mathbb{F}_{q^2})$ we have $\mathcal{O}_C((q+1)P) \cong \mathcal{O}_C(1)$. Hence for any $P, Q \in C(\mathbb{F}_{q^2})$ there is $f \in K(C)$ such that $(f) = (q+1)P - (q+1)Q$. Hence $\mathcal{O}_C(G) \cong \mathcal{O}_C(G') \cong \mathcal{O}_C(c)(-E)$ and for any $B \subseteq C(\mathbb{F}_{q^2}) \setminus \{P_1, \dots, P_s\}$ the codes $\mathcal{C}(B, G)$ and $\mathcal{C}(B, G')$ are isometric. We will denote with $\mathcal{C}(B, \mathcal{O}_C(c)(-E))$ any of these codes and with $\mathcal{C}(B, \mathcal{O}_C(c)(-E))^\perp$ their dual.

Lemma 5. Fix integers $d \geq 1$, $s \geq 1$ and $a_i \in \{1, \dots, q+1\}$, $1 \leq i \leq s$, with $a_1 \leq \dots \leq a_s$. Let r be the maximal integer $i \leq s$ such that $a_i \leq d - s + r$. Set $d' := d - s + r$. Set $a'_i := a_i$ for $i \leq r$. Fix s distinct $P_1, \dots, P_s \in C(\mathbb{F}_{q^2})$. Set $E := \sum_{i=1}^s a_i P_i$ and $E' := \sum_{i=1}^r a_i P_i$. Fix any $B \subseteq C(\mathbb{F}_{q^2}) \setminus \{P_1, \dots, P_s\}$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(d)(-E))$ and $\mathcal{C}' := \mathcal{C}(B, \mathcal{O}_C(d')(-E'))$. Then codes \mathcal{C} and \mathcal{C}' are isometric. Hence their dual codes are isometric.

Proof. If $r = s$, then $d' = d$, $E' = E$ and hence there is nothing to prove. Assume $r < s$, i.e. $a_r > d$. Set $E'' := \sum_{i=1}^r b_i P_i$ with $b_i = a_i$ if $a_i \leq d$ and $b_i = q+1$ if $a_i \geq d+1$. Set $\mathcal{C}'' := \mathcal{C}(B, \mathcal{O}_C(d)(-E''))$. Fix any $h \in H^0(C, \mathcal{O}_C(d)(-E))$ and represent h by a degree d homogeneous polynomial $h_1 \in \mathbb{F}_{q^2}[x_0, x_1, x_2]$ vanishing on the zero-dimensional scheme $E \subset \mathbb{P}^2$. Fix any $i \in \{1, \dots, s\}$ such that $a_i \geq d+1$. Lemma 3 gives that h_1 is divided by the equation ℓ of the tangent line L_{C, P_i} to C at P_i . Since ℓ has order of contact $q+1 \geq a_i$ with C at P_i , we get that $(b_i - a_i)P_i$ is a base-divisor of $H^0(C, \mathcal{O}_C(d)(-E))$. Since this is true for all $i > r$, we get $H^0(C, \mathcal{O}_C(d)(-E)) = H^0(C, \mathcal{O}_C(d)(-E''))$. Since $B \cap \{P_1, \dots, P_s\} = \emptyset$ and $E'' - E$ is supported by P_1, \dots, P_s , the codes \mathcal{C} and \mathcal{C}'' are isometric. We have $\mathcal{O}_C(b_i P_i) = \mathcal{O}_C((q+1)P_i) \cong \mathcal{O}_C((q+1)P_1)$ for every $i > r$ and in this isomorphism only divisors with support P_1 and B are involved. Since $P_1 \notin B$ and $P_i \notin B$, the codes \mathcal{C}'' and \mathcal{C}' are isometric. \square

4. PROOFS OF THE MAIN RESULTS

Proof of Theorem 1. We have $n = \sharp(B) = q^3 - 2$. Since $d \leq q < \deg(C)$, we have $h^0(C, \mathcal{O}_C(d)) = \binom{d+2}{2}$. If, say, $a_1 \geq a_2 \geq a_3$, the assumptions $a_1 \leq d$

and $a_1 + a_2 + a_3 \leq 3d - 1$ give $a_i \leq d + 2 - i$ for all i . Hence Lemma 4 gives $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$. Hence $h^0(C, \mathcal{O}_C(d)(-E)) = \binom{d+2}{2} - a_1 - a_2 - a_3 = k$. Since $\sharp(B) > d \cdot \deg(C)$, no element of $H^0(C, \mathcal{O}_C(d))$ vanishes at all points of B . Hence \mathcal{C} is an $[n, k]$ -code.

By Lemma 1 it is sufficient to prove that $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup A}(d)) = 0$ for all $A \subset B$ such that $\sharp(A) \leq d - 1$ and that for any $S \subset B$ such that $\sharp(S) = d$ we have $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$ if and only if $S \subset L_i$ for some i .

Each line L_i contains $q - 1$ points of B , while $\deg(E \cap L_i) = 2$. Hence for any $S \subseteq L_i \cap B$ with $\sharp(S) = d$ we have $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$ (see the first lines of the proof of Lemma 2 or see the easy “if” part of Lemma 2, (b)).

Let E_i be the divisor of C with degree a_i and P_i as its support. Hence $E = E_1 \sqcup E_2 \sqcup E_3$. Fix a set $S \subset B$ such that $\sharp(S) \leq d$ and assume $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$. We have $S \cap \{P_1, P_2, P_3\} = \emptyset$ and $\deg(E \cup S) = a_1 + a_2 + a_3 + \sharp(S)$.

Since $a_1 + a_2 + a_3 + \sharp(S) \leq 4d - 5$, we may apply Lemma 2 to the scheme $E \cup S$. Let $T \subset \mathbb{P}^2$ be the curve arising in the statement of Lemma 2. Set $x := \deg(T) \in \{1, 2, 3\}$. Set $e_i := \deg(T \cap E_i)$, $1 \leq i \leq 3$. We have $0 \leq e_i \leq a_i$. If $e_i \geq x + 1$, then Lemma 3 gives $L_{C, P_i} \subseteq T$. Assume $e_i \leq x$ for all i . For $x = 2$ we get $\deg(T \cap (E \cup S)) \leq d + 6 \leq 2d + 1$. For $x = 3$ we get $\deg(T \cap (E \cup S)) \leq d + 9 \leq 3d - 1$. If $x = 1$ we may have $e_i > 0$ only for at most two indices, say $i = 1, 2$. Since $\sharp(S) \leq d$, we get $\sharp(S) + e_1 + e_2 \geq d + 2$ and $\sharp(S) + e_1 + e_2 = d + 2$ if and only if $T = L_3$, $S \subset L_3 \cap B$ and $\sharp(S) = d$.

Now assume that T contains one of the lines L_{C, P_i} , say L_{C, P_1} . Let T' be the curve whose equation is obtained dividing an equation of T by an equation of L_{C, P_1} . We have $\deg(T') = x - 1$, $T' + L_{C, P_1} = T$ as divisors of \mathbb{P}^2 and $T = L_{C, P_1} \cup T'$ as sets. Since $L_{C, P_1} \cap B = \emptyset$, we have $T \cap S = T' \cap S$ and $\deg(T \cap (E \cup S)) = \deg(T' \cap (E_2 \cup E_3 \cup S))$.

(a) If $x = 1$, we get $T \cap S = \emptyset$. We also get $\deg(T \cap E) = a_1 \leq d$, absurd.

(b) Assume $x = 2$. Hence T' must be a line such that $\deg(T' \cap (E_2 \cup E_3 \cup S)) \geq 2d + 2 - a_1$. If either $T' = L_{C, P_2}$ or $T' = L_{C, P_3}$, we get $T' \cap S = \emptyset$ and $\deg(T' \cap (E_2 \cup E_3 \cup S)) \leq \max\{e_2, e_3\} \leq d$, a contradiction. If neither $T' = L_{C, P_2}$ nor $T' = L_{C, P_3}$, then $\deg(T' \cap E_2) \leq 1$, $\deg(T' \cap E_3) \leq 1$ and $\deg(T' \cap (E_2 \cup E_3)) = 2$ if and only if $T' = L_1$. Since $\sharp(S) \leq d$, we get $\deg(T \cap (E \cup S)) \leq a_1 + 2 + \sharp(S)$ with equality only if $T' = L_1$ and $S \subset L_1$. Since $\deg(T \cap (E \cup S)) \geq 2d + 2$ by assumption, we get $\sharp(S) = d$ and $S \subset L_1$, as wanted.

(c) Now assume $x = 3$. We get $\deg(T' \cap (E_2 \cup E_3 \cup S)) \geq 3d - a_1$. T' is a conic. If neither L_{C, P_2} nor L_{C, P_3} is a component of T , then Lemma 3 gives $e_2 \leq 2$ and $e_3 \leq 2$ and hence $\sharp(T' \cap S) \geq 3d - 4 - a_1 \geq 2d - 4 > d$. If, say, T' contains L_{C, P_2} and T'' is the line with $T' = T'' + L_{C, P_2}$, then we get $\sharp((S \cup E_3) \cap T'') \geq 3d - a_1 - a_2$. Since $a_1 + a_2 \leq 2d - 1$, we get $\deg(T'' \cap (E_3 \cup S)) \geq d + 1$. Since $\deg(T'' \cap E_3) \leq 1$, we get $a_1 + a_2 = 2d - 1$, say $a_1 = d$, $a_2 = d - 1$ and that S is formed by d points on a line T'' through P_3 . If either $T'' = L_1$ or $T'' = L_3$, then we are done. In any case it is sufficient to prove that the case $x = 3$ of Lemma 2 does not apply, i.e. that $E_1 \cup E_2 \cup \{P_3\} \cup S$ is not the complete intersection of $T = L_{C, P_1} \cup L_{C, P_2} \cup T''$ and a degree d curve, J . Since $a_2 = d - 1$, E_2 is not the complete intersection of L_{C, P_2} and J , while $L_{C, P_2} \cap (\{P_3\} \cup S) = \emptyset$, absurd. \square

Remark 3. Take the set-up of Theorem 1 and assume $d \geq 6$, $a_1 = a_2 = d$ and $1 \leq a_3 \leq d - 5$. Take any line L through P_3 with $L \neq L_{C, P_3}$ and any $S \subset L \cap B$ such that $\sharp(S) = d$. We claim that S is the support of a codeword of \mathcal{C}^\perp with weight d .

Lemma 4 gives $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$. Hence to prove the claim it is sufficient to prove $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$. It is sufficient to prove $h^1(\mathbb{P}^2, \mathcal{I}_{E_1 \cup E_2 \cup \{P_3\} \cup S}(d)) > 0$. Since $\deg(E_1 \cup E_2 \cup \{P_3\} \cup S) = 3d + 1$ and $E_1 \cup E_2 \cup \{P_3\} \cup S$ is contained in the degree 3 curve $L_{C, P_1} \cup L_{C, P_2} \cup L$, we may apply the (easy) “if” part of Lemma 2, (e).

Remark 4. Take the set-up and assumptions of Theorem 1, but only assume $a_1 + a_2 + a_3 \leq 3d - 4$. In this case we get that \mathcal{C}^\perp has minimum distance d and that each codeword supported by d points of some L_i , $i = 1, 2, 3$, has minimum weight.

Proof of Theorem 3. Since $\sharp(L_i \cap C(\mathbb{F}_{q^2})) = q + 1$ for all i , we have $\sharp(C(\mathbb{F}_{q^2}) \cap (L_1 \cup L_2 \cup L_3)) = 3q$. Hence $\sharp(B') = q^3 - 3q + 1$. Lemma 4 gives $h^0(C, \mathcal{O}_C(d)(-E)) = \binom{d+2}{2} - a_1 - a_2 - a_3$. Since $E \subset C$ and $\sharp(B') + \deg(E) > d \cdot \deg(C)$, no non-zero element of $H^0(C, \mathcal{O}_C(d)(-E))$ vanishes at all points of B' . Hence $k = \binom{d+2}{2} - a_1 - a_2 - a_3$.

Theorem 1 implies that \mathcal{C}^\perp has minimum distance at least $d + 1$. The set of all lines through P_i has cardinality $q^2 + 1$. One of these lines is the tangent line L_{C, P_i} and two of these lines are L_j and L_h , $\{i, j, h\} = \{1, 2, 3\}$. Hence $\sharp(\mathcal{S}) = 3(q^2 - 2)$. Since $\sharp(B' \cap L) = q$ for all $L \in \mathcal{S}$, we have $\sharp(\mathcal{S}(d + 1)) = 3(q^2 - 2) \binom{q}{d+1}$. Fix any $S \in \mathcal{S}(d + 1)$. We have $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$ (Lemma 4). Parts (a) and (b) of Lemma 2 give $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) = 1$. Hence Lemma 1 gives that S is the support of a unique (up to a non-zero scalar) codeword with minimum weight. Now assume $d \geq 6$ and $a_1 + a_2 + a_3 \leq 3d - 6$. Look at the proof of Theorem 1. Fix any $S \subset B'$ such that $\sharp(S) = d + 1$. Since $a_1 + a_2 + a_3 + \sharp(S) \leq 4d - 5$, we may apply Lemma 2 and get a curve T . Set $x := \deg(T) \in \{1, 2, 3\}$ and $e_i := \deg(E_i \cap T)$. First assume $L_{C, P_i} \not\subset T$ for all i . If $x = 1$, then we get $\deg(E \cap T) \leq 1$ and $\deg(E \cap T) > 0$ if and only if $P_i \in T$. Since $S \cap T \neq \emptyset$, we get $T \in \mathcal{S}$ and $S \in \mathcal{S}(d + 1)$. If $x = 2$, then we have $e_1 + e_2 + e_3 \leq 6$. Since $\deg(T \cap (E \cup S)) \geq 2d + 2$, we get $d + 7 \geq 2d + 2$, a contradiction. Now assume $x = 3$. Since $\deg(T \cap (E \cup S)) \geq 3d$ and $e_i \leq 3$ for all i , we get $d \leq 5$, a contradiction. From now on we assume $L_{C, P_i} \subset T$ for some i and write $T = L_{C, P_i} + T'$. In the case $x = 1$ we obviously get a contradiction. In the case $x = 2$ we get a contradiction, because $\deg((S \cup E_j \cup E_h) \cap T') \leq \sharp(S) + 1$ ($\{i, j, h\} = \{1, 2, 3\}$), because $L_i \cap B' = \emptyset$. Now assume $x = 3$ and that no L_{C, P_j} , $j \neq i$, is contained in T' . Hence $e_j + e_h \leq 4$, $\{i, j, h\} = \{1, 2, 3\}$. We get $a_i + 4 + d + 1 \geq 3d$, a contradiction. Now assume $L_{C, P_j} \subset T'$, say $T' = R + L_{C, P_j}$. We use the last part of the proof of Theorem 1 with, now, $\sharp(S) = d + 1$, but with $a_1 + a_2 \leq 2d - 2$. \square

Lemma 6. Fix the set-up of Theorem 2 and set $E_i := a_i P_i$, $E'_i := (a_i - 1)P_i$, $E := \cup_{i=1}^s E_i$ and $E' := \cup_{i=1}^s (a_i - 1)P_i$. E and E' are effective divisor on C with degree $a_1 + \dots + a_s$ and $a_1 + \dots + a_s - s$. We see them as zero-dimensional subschemes of \mathbb{P}^2 . Fix any $S \subset B$. For any integer t we have an exact sequence of coherent sheaves:

$$(3) \quad 0 \rightarrow \mathcal{I}_{E' \cup (S \setminus R \cap S)}(t - 1) \rightarrow \mathcal{I}_{E \cup S}(t) \rightarrow \mathcal{I}_{\{P_1, \dots, P_s\} \cup (S \cap R)}(t) \rightarrow 0$$

in which $\{P_1, \dots, P_s\} \cup (S \cap R)$ is a set of $s + \sharp(S \cap R)$ points of R . For each integer $i \geq 0$ we have

$$(4) \quad h^i(\mathbb{P}^2, \mathcal{I}_{E \cup S}(t)) \leq h^i(\mathbb{P}^2, \mathcal{I}_{E' \cup (S \setminus R \cap S)}(t - 1)) + h^i(R, \mathcal{I}_{\{P_1, \dots, P_s\} \cup (S \cap R), R}(t))$$

If $t \geq \sharp(S \cap R) + s - 1$, then $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(t)) \leq h^1(\mathbb{P}^2, \mathcal{I}_{E' \cup (S \setminus R \cap S)}(t - 1))$.

Proof. For any closed subscheme $Z \subset \mathbb{P}^2$ the zero-dimensional scheme $\text{Res}_L(Z)$ is the closed subscheme of \mathbb{P}^2 with $\mathcal{I}_Z : \mathcal{I}_R$ as its ideal sheaf. For any finite set $A \subset \mathbb{P}^2$ we have $\text{Res}_R(S) = S \setminus S \cap R$. Since R is a degree 1 divisor of \mathbb{P}^2 we have the residual sequence

$$(5) \quad 0 \rightarrow \mathcal{I}_{\text{Res}_R(Z)}(t-1) \rightarrow \mathcal{I}_Z(t) \rightarrow \mathcal{I}_{Z \cap R, R}(t) \rightarrow 0$$

Take $Z := E \cup S$ with $S \subset B$. We have $\text{Res}_R(S) = S \setminus S \cap R$. Since R is not tangent to C and $P_i \in R$ for all i , we have $\text{Res}_R(E) = E'$. Hence $\text{Res}_R(E \cup S) = E' \cup (S \setminus S \cap R)$. Since $P_i \in R$ for all i and R is transversal to C , we have $R \cap E = \{P_1, \dots, P_s\}$ and hence $R \cap (E \cup S) = \{P_1, \dots, P_s\} \cup (S \cap R)$. Applying (5) we get (3). The cohomology exact of (3) gives (4). Since $R \cong \mathbb{P}^1$ and $\deg(\{P_1, \dots, P_s\} \cup (S \cap R)) = s + \sharp(S \cap R)$, we have $h^1(R, \mathcal{I}_{\{P_1, \dots, P_s\} \cup (S \cap R), R}(t)) = 0$ if $t \geq s + \sharp(S \cap R) - 1$. Hence $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(t)) \leq h^1(\mathbb{P}^2, \mathcal{I}_{E' \cup (S \setminus S \cap R), R}(t))$ if $t \geq s + \sharp(S \cap R) - 1$. \square

Proof of Theorem 2. The parameters n, k are obvious (Lemma 4 and the inequality $\deg(E) + \sharp(B) > d \cdot \deg(C)$).

Lemma 4 gives $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$. By Lemma 1 it is sufficient to prove that $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup A}(d)) = 0$ for all $A \subset B$ such that $\sharp(A) \leq d + 1 - s$ and that for any $S \subset B$ such that $\sharp(S) = d + 2 - s$ we have $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$ if and only if $S \subset R$. If $S \subset B \cap R$ and $\sharp(S) = d + 2 - s$, then $\deg((E \cup S) \cap R) = d + 2$. Hence part (b) of Lemma 2 gives $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$. Hence the “if” part of Theorem 2 is proved.

Now we check the “only if” part. Fix $S \subset B$ such that $\sharp(S) \leq d + 2 - s$ and $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$. Since $\deg(E \cup S) \leq 4d - 5$, we may apply Lemma 2. Let T be any curve as in (b), (c) or (d) of Lemma 2. Set $x := \deg(T)$. Set $E_i := a_i P_i$, $e_i := \deg(E_i \cap T)$ and $f := \sharp(S \cap T)$. Notice that if R is not a component of T , then $e_i > 0$ for at most x indices. Set $E^{(i)} := E \setminus E_i$ and $E' := \sum_{i=1}^s (a_i - 1) P_i$. See E' both as a positive divisor of C and a zero-dimensional subscheme of \mathbb{P}^2 . We have $\deg(E') = \deg(E) - s$. Seen E as a subscheme of \mathbb{P}^2 we defined the scheme $\text{Res}_R(E) \subseteq E \subset \mathbb{P}^2$ (proof of Lemma 6). Since R is transversal to C at each P_i , we have $E' = \text{Res}_R(E)$.

(a) In this step we assume that T contains no tangent line L_{C, P_i} , $1 \leq i \leq s$. Hence $e_i \leq x$ for all i (Lemma 3). Hence $\deg((E \cup S) \cap T) \leq sx + f$. First assume $x = 1$. We get $\sharp(\{P_1, \dots, P_s\} \cap T) + f \geq d + 2$ and hence $S \subset T$, $P_i \in T$ for all i (i.e. $T = R$) and $f = d + 2 - s$, as wanted. Now assume $x = 2$ and that R is not a component of T . We get $2 \cdot 2 + (d + 2 - s) \geq 2d + 2$, a contradiction. Now assume that $x = 2$ and that R is a component of T , say $T = R \cup L'$. If $\sharp(S \cap R) \geq d - s + 1$, the $S \subset R \cap B$, as wanted; if $\sharp(S \cap R) \leq d - s$, then $\deg(L' \cap (E' \cup (S \setminus S \cap R))) \geq d + 2 + s \geq d + 2$. Since $L' \neq L_{C, P_i}$ for any i and $L' \neq R$, we have $\deg(E' \cap L') \leq 1$. Hence $\sharp(S) \geq \sharp(S \cap L') \geq d + 1$, absurd. If $x = 3$ and R is not a component of T , then we get $3 \cdot 3 + d + 2 - s \leq 3d - 1$, a contradiction. Now assume $x = 3$ and $T = R \cup T'$. We may assume $f \leq d + 1 - s$. Hence $\deg(T' \cap (E' \cup (S \setminus S \cap R))) \geq 3d - (d + 1 - s) = 2d - 1 + s$. Since $2d - 1 + s \geq 2d + 2$, we get a contradiction as in the case $x = 2$.

(b) Now assume that T contains one of the tangent lines L_{C, P_i} . If $x = 1$, then $L_{C, P_i} = T$ and hence $\deg(T \cap (E \cup S)) = e_i \leq d$, absurd. Now assume $x \geq 2$ and write $T = T' \cup L_{C, P_i}$. We have $T \cap (E \cup S) = E_i \sqcup T' \cap (S \cup E^{(i)})$. Assume for the moment that T' contains no tangent line to C at one of the points P_j , $j \neq i$. We get $e_j \leq x - 1$ for all $j \neq i$ (Lemma 3). Hence $\deg(T \cap (E \cup$

$S)) = e_i + \deg(T' \cap (S \cup E^{(i)})) \leq e_i + f + (x-1)(s-1)$. First assume $x = 2$. Since $e_i \leq d$, we get $f + (s-1) \geq d+2$, a contradiction. Now assume $x = 3$, i.e. $\deg(T') = 2$. First assume $R \subset T'$, say $T' = R \cup L''$ with L'' a line. If $\sharp(S \cap R) \geq d+2-s$, then we are done. Hence we may assume $\sharp(S \cap R) \leq d+1-s$. Hence $\deg(L'' \cap ((S \setminus S \cap R) \cup E)) \geq 3d - e_i - (d+1-s) \geq d+2$. Since $L'' \neq R$ and $L'' \neq L_{C,P_j}$ for any j , we have $\deg(E \cap L'') \leq 1$. Hence $\sharp(S) \geq d+1$, absurd. Now assume $R \not\subset T'$. Since the points P_1, \dots, P_s are collinear, Bezout theorem gives $\sharp(T' \cap \{P_1, \dots, P_s\}) \leq 2$. Hence Lemma 3 gives $\deg(E^{(i)} \cap T') \leq 4$. Hence $f \geq 3d-1-a_i-4 \geq 2d-5 > d+2-s$, absurd. Now assume the existence of $j \neq i$ such that T' contains a tangent line L_{C,P_j} , $j \neq i$. We have $L_{C,P_j} \cap B = \emptyset$. Hence $f = 0$ if $x = 2$, absurd. Now assume $x = 3$ and write $T' = L_{C,P_j} \cup L$ with L a line and $\sharp(S \cap L) = f$. If L is a tangent line to C , say at P , then either $\deg((E \cup S) \cap T) = e_i + e_j + e_h$ (case $P = P_h$ with $h \in \{1, \dots, s\} \setminus \{i, j\}$ or $\deg((E \cup S) \cap T) \leq e_i + e_j + 1$ (case $P \notin \{P_1, \dots, P_s\}$). We get a contradiction, because $e_i + e_j + e_h \leq 3d-1$ if i, j, h are distinct. If $L \neq L_{C,P_h}$, $h \notin \{i, j\}$, then $\deg(((E \setminus (E_i \cup E_j)) \cup S) \cap L) \leq f+1$ and equality holds if and only if $P_h \in L$ for some $h \notin \{i, j\}$. Since $f \leq d+1-s$, we get $e_i + e_j + d+2-s \geq 3d$, a contradiction. \square

Theorem 4. *Take the set-up of Theorem 2, but assume $a_1 + \dots + a_s \leq 3d-6$ and $a_i + a_j \leq 2d-2$ for all $i \neq j$. Set $B_1 := C(\mathbb{F}_{q^2}) \setminus R \cap C(\mathbb{F}_{q^2})$. Set $\mathcal{C} := \mathcal{C}(B_1, \mathcal{O}_C(d)(-E))$. Then \mathcal{C} is an $[n, k]$ code with $n = q^3 - q$ and $k = \binom{d+2}{2} - a_1 - \dots - a_s$. Let \mathcal{S} be the set of all lines $\neq R$, containing one of the points P_1, \dots, P_s and not tangent to C . Let $\mathcal{S}(d+1)$ be the set of all $S \subset B_1$ such that $\sharp(S) = d+1$ and $S \subset L$ for some $L \in \mathcal{S}$. We have $\sharp(\mathcal{S}(d+1)) = s(q^2-1)\binom{q}{d+1}$. The dual code \mathcal{C}^\perp has minimum distance $d+1$ and for each $S \in \mathcal{S}(d+1)$ there is a unique (up to a non-zero constant) codeword with minimum weight with S as its support. Moreover, all codewords of \mathcal{C}^\perp with minimum weight are associated to a unique $S \in \mathcal{S}(d+1)$.*

Proof. The parameters n, k of \mathcal{C} are obvious, because $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$ by Lemma 4 and the inequality $\deg(E) + \sharp(B_1) > d \cdot \deg(C)$ holds. If $A \in \mathcal{S}(d+1)$, then the “if” part of Lemma 2 gives $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup A}(d)) > 0$. Hence to prove the theorem (including that if $A \in \mathcal{S}(d+1)$, then $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup A}(d)) = 1$ and A is the support of a unique (up to a scalar) codeword with minimum weight) it is sufficient to prove the following Claim. Take any $S \subset B_1$ such that $\sharp(S) \leq d+1$ and $h^1(\mathcal{I}_{E \cup S}(d)) > 0$.

Claim: We claim that $S \in \mathcal{S}(d+1)$.

Proof of the Claim: We use the notation $E_i, E^{(i)}, E'$, and so on, introduced in the proof of Theorem 2. Since $\deg(E \cup S) = a_1 + \dots + a_s + \sharp(S) \leq 4d-5$, we may apply Lemma 2 and get a curve $T \subset \mathbb{P}^2$. Set $x := \deg(T) \in \{1, 2, 3\}$. Set $e_i := \deg(T \cap E_i)$ and $f := \sharp(T \cap S)$. Let $L \subset \mathbb{P}^2$ be any line. We have $\deg(L \cap (E \cup S)) = s$ if $L = R$, $\deg(L \cap (E \cup S)) = a_i$ if $L = L_{C,P_i}$, $\deg(L \cap E) = 1$ if $L \neq R$, L is not tangent to C and $L \cap \{P_1, \dots, P_s\} \neq \emptyset$, while $L \cap E = \emptyset$ if $L \cap \{P_1, \dots, P_s\} = \emptyset$.

(i) Here we assume that R is not an irreducible component of T . First assume that no L_{C,P_i} is a component of T . Hence $e_i \leq x$ for all i (Lemma 3). If $x = 1$ we get $S \subset T$, $\sharp(S) = d+1$ and $L \cap \{P_1, \dots, P_s\} \neq \emptyset$ (i.e. $T \in \mathcal{S}$ and $S \in \mathcal{S}(d+1)$), because $s = \deg((E \cup S) \cap R) = s < d+2$. Now assume $x = 2$ (resp. $x = 3$). Since the points P_1, \dots, P_s are collinear and $R \not\subset T$, Bezout theorem gives $\sharp(\{P_1, \dots, P_s\} \cap T) \leq x$. Hence $2 \cdot 2 + \sharp(S) \geq 2d+2$ (resp. $3 \cdot 3 + \sharp(S) \geq 3d$), a contradiction. Now assume,

say, $L_{C,P_i} \subseteq T$ and set $T = L_{C,P_i} \cup T'$ with $S \cap T = S \cap T'$ and $\deg(T') = x - 1$. If $x = 1$, then we get $\deg((E \cup S) \cap T) = a_i < d + 2$, absurd. If $x = 2$, then we get $a_i + (\deg(E^{(i)} \cup S) \cap T') \geq 2d + 2 - a_1 \geq d + 2$. Hence $S \subset T'$, $T' \in \mathcal{S}$ and $S \in \mathcal{S}(d + 1)$. Now assume $x = 3$ and that T' contains no L_{C,P_j} , $j \neq i$. We get $\deg(T' \cap E^{(i)}) \leq \deg(T')^2 = 4$. Since $\sharp(S) \leq d + 1$, we get $\deg(T \cap (E \cup S)) \leq a_i + 4 + d + 1 < 3d$, absurd. Now assume $L_{C,P_j} \subset T$ for some $j \neq i$. We still have $a_i + a_j + d + 1 < 3d$ (and hence a contradiction), because we assumed $a_i + a_j \leq 2d - 2$ for all $i \neq j$.

(ii) Now assume that R is an irreducible component with multiplicity $c \geq 1$ of T and write $T = cR + T_1$ with $\deg(T_1) = x - c$. Since $R \cap B_1 = \emptyset$, we have $f = \sharp(S \cap T_1)$. Hence $x > c$. Now assume $x = 2$ and hence $c = 1$. We get $\deg(T_1 \cap (S \cup E)) \geq 2d + 2 - s \geq d + 3$, absurd. Now assume $x = 3$ and $c = 2$. We get $\deg(T_1 \cap (E \cup S)) \geq 3d - 2s \geq d + 2$. Hence $T_1 \in \mathcal{S}$ and $S \in \mathcal{S}(d + 1)$. Now assume $x = 3$ and $c = 1$. If T_1 contains no tangent line L_{C,P_i} , then $\deg(T_1 \cap E) \leq 2 \cdot 2$. Hence $3d \leq \deg(T \cap (E \cup S)) \leq s + \deg(T_1 \cap (E \cup S)) \leq s + 4 + d + 1$, absurd. Now assume $L_{C,P_i} \subset T_1$, say $T_1 = L_{C,P_i} \cup T_2$. Set $E''[i] := \sum_{j \neq i} (a_j - 1)P_j$. We have $E''[i] = \text{Res}_R(E^{(i)})$. We get $3d \leq \deg(T \cap (E \cup S)) = (a_i - 1) + s + \deg(T_2 \cap (S \cup E''[i])) \leq s + a_i - 1 + d + 2$, absurd. \square

REFERENCES

- [1] Bernardi A., Gimigliano A., Idà M.: Computing symmetric rank for symmetric tensors. *J. Symbolic. Comput.* **46**(1), 34–53 (2011).
- [2] Couvreur A.: The dual minimum distance of arbitrary dimensional algebraic-geometric codes. arXiv:0905.2345v3, *J. Algebra* (to appear).
- [3] Ellia Ph., Peskine Ch.: Groupes de points de \mathbf{P}^2 : caractère et position uniforme. *Algebraic geometry (L'Aquila, 1988)*, 111–116, *Lecture Notes in Math.*, 1417, Springer, Berlin (1990).
- [4] Fontanari C., Marcolla C.: On the geometry of small weight codewords of dual algebraic geometric codes. arXiv:1104.1320v1.
- [5] Hirschfeld J. P. W.: *Projective geometries over finite fields*. Clarendon Press, Oxford (1979).
- [6] Homma M., Kim S. J.: Toward the determination of the minimum distance of two-point codes on a Hermitian curve. *Des. Codes Cryptogr.* **37**(1), 11–132 (2005).
- [7] Homma M., Kim S. J.: The two-point codes on a Hermitian curve with the designed minimum distance. *Des. Codes Cryptogr.* **38**(1), 55–81 (2006).
- [8] Homma M., Kim S. J.: The two-point codes on a Hermitian curve with the designed minimum distance in even characteristic. *Des. Codes Cryptogr.* **39**(3), 375–386 (2006).
- [9] Homma M., Kim S. J.: The complete determination of the minimum distance of two-point codes on a Hermitian curve. *Des. Codes Cryptogr.* **40**(1), 5–24 (2006).
- [10] Homma M., Kim S. J.: The second generalized Hamming weight for two-point codes on a Hermitian curve. *Des. Codes Cryptogr.* **50**(1), 1–40 (2009).
- [11] Matthews G. L.: The Weierstrass semigroup of an m -tuple of collinear points on a Hermitian curve. *Finite fields and applications*, 12–24, *Lecture Notes in Comput. Sci.*, 2948, Springer, Berlin (2004).
- [12] Munuera C.: On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory* **40**, 2092–2099 (1994).
- [13] Munuera C., Ramirez D.: The second and third generalized Hamming weights of Hermitian codes. *IEEE Trans. Inform. Theory* **45**(2), 709–712 (1999).
- [14] Park S.: Minimum distance of Hermitian two-point codes, *Des- Codes. Cryptogr.* **57**, 195–213 (2010).
- [15] Pellegrini M., Marcolla C., Sala S.: On the weights of affine-variety codes and some Hermitian codes, *WCC 2011 - Workshop on coding and cryptography* 273–282 (2011).
- [16] Ravagnani A.: Master thesis, University of Trento, in preparation.
- [17] Stichtenoth H.: *Algebraic Function Fields and Codes*. Springer, Berlin (1993).

- [18] Yang K., Kumar P. V.: On the true minimum distance of Hermitian codes, in: “ Coding theory and algebraic geometry ”. Lect. Notes in Math. 1518, pp. 99–107, Springer, Berlin, 1992.
- [19] Yang K., Kumar P. V., H. Stichtenoth H.: On the weight hierarchy of geometric Goppa codes. IEEE Trans. Inform. Theory **40**, 913–920 (1994).

DEPT. OF MATHEMATICS, UNIVERSITY OF TRENTO, 38123 POVO (TN), ITALY
E-mail address: `ballico@science.unitn.it`

UNIVERSITY OF TRENTO, 38123 POVO (TN), ITALY
E-mail address: `alberto.ravagnani@unitn.it`